ICS CYBERSECURITY FOR THE C-LEVEL

Cyber threats against Industrial Control Systems (ICS) continue to increase in intensity, frequency, and complexity. Yet, basic cybersecurity practices within many ICS organizations continue to be an afterthought or significantly less than needed. This document was developed as a tool to help facilitate the communication of strong, basic cybersecurity principles to the leadership of ICS organizations.

Through conversation with various stakeholders, the need for a document that conveys concise cybersecurity concepts and strategies to organizational leadership became apparent. Thus, the U.S. Department of Homeland Security's (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT), with direction from the Industrial Control System Joint Working Group (ICSJWG), developed this document to support communication and improve cybersecurity practices across the Nation's critical infrastructure (CI).

ICS ATTACKS - GROWING SOPHISTICATION

Attacks that target ICS infrastructure continue to evolve and mature. Through a variety of methods, malicious threat actors are introducing sophisticated malware into control systems at growing rates. The following case studies, Havex and BlackEnergy, represent sophisticated, global malware campaigns against ICS that went unnoticed for years. These examples evidence the ability of threat actors to remotely issue command functions via malicious code.

HAVEX

Sophisticated threat actors using Havex malware have targeted and compromised control systems worldwide since 2013. Spear phishing along with infected ICS software downloads from legitimate websites have been the main attack vectors. The Havex malware operates as a Remote Access Trojan (RAT) with the ability to inject unauthorized control commands as well as cause a denial of service effect on certain applications.

BLACKENERGY

The BlackEnergy campaign used previously unknown software vulnerabilities in multiple common Human Machine Interface (HMI) software products to gain direct access to control system operating screens. Since 2011, BlackEnergy has infected dozens of control systems in the U.S. and hundreds globally. The malicious code could potentially be used to manipulate control processes and cause physical damage. No interaction with the target was required as BlackEnergy targeted systems connected **directly to the internet.**

LONG-TERM THREAT

These two campaigns illustrate a concerted effort by sophisticated threat actors for at least four years to understand critical ICS, discover unknown/ unpatched vulnerabilities for exploitation, and use differing techniques to gain access to the operational environment.

SIX QUESTIONS EVERY C-LEVEL EXECUTIVE SHOULD BE ASKING

1) What's at Risk – have we prioritized our assets and identified the potential consequences if our control system was compromised? Can we sustain operations of critical processes following a cyber incident?

2) Who is the manager ultimately responsible for cybersecurity or do we rely on third-party support?

3) Is our ICS environment protected from the Internet and how have we validated that?

4) Do we have remote access to our ICS network? If so, why do we need it, and how is it protected and monitored?

5) Do we have an ICS-CERT Portal Account to receive alerts and advisories?

6) Are we reading available resources and applying the recommended cybersecurity best practices?

Homeland Security

KEY RISK MANAGEMENT CONCEPTS

Identify Critical Assets – Assess the Risk
Complete a risk assessment to ascertain areas of greatest vulnerability, identify critical assets, and define the parameters for your security plan. Perform a baseline cybersecurity assessment via NIST's "Guide to Industrial Control Systems (ICS) Security" or DHS' Cyber Security Evaluation Tool (CSET).

Assign a Manager Responsible for Cybersecurity
Every organization needs a trained and qualified individual whose primary responsibility is cyber-security. A cybersecurity manager should set policies and implement procedures, enforce monitoring and protective/detective controls, train employees, perform regular assessments, and implement patching and configuration practices.

Protect Your Networks from the Internet
Do NOT allow direct connectivity from the internet to your ICS network. Protect your network from remote access via defensive measures, monitoring, and strong authentication requirements. Isolate, protect, and monitor your key assets.

Limit the Use of Remote Access to Your ICS
If remote access is required, protect your ICS with multiple defensive layers. Consider using different levels of access and appropriate controls for remote access, coupled with strong detection/ monitoring capabilities. Implement a control system demilitarized zone (DMZ) with two-factor authentication and a virtual private network (VPN) connection.

Join the ICS-CERT Portal
Joining the ICS-CERT Portal allows access to alerts and advisories, indicators of compromise, and a secure method of reporting cyber incidents and requesting incident response services.

Take Advantage of Available Resources
Participate in your sector's Information Sharing and Analysis Center (ISAC) information sharing programs, know your Sector Specific Agency (SSA), and visit the ICS-CERT website.

ICS-CERT RESOURCES AND ASSISTANCE

ICS-CERT operates within the National Cybersecurity and Communications Integration Center (NCCIC), a division of the DHS Office of Cybersecurity and Communications (CS&C). NCCIC/ICS-CERT is an integral component of the DHS Strategy for Securing Control Systems and strives to reduce risks and threats to CI by collaborating with other government and private sector partners.

ICS-CERT provides or sponsors the following services and activities to improve CI security:

- **OUTREACH AND TRAINING** – ICS-CERT performs outreach activities to help CI sectors understand cybersecurity risks and offers training opportunities to assist the control systems community in improving their cybersecurity preparedness.
- **ICSJWG** – The ICSJWG facilitates partnerships between the Federal government and private sector owners and operators in all CI sectors through biannual face-to-face meetings, webinars, and newsletters.
- **CSET** – CSET is a desktop software tool that enables users to self-assess their network and ICS security practices against recognized standards, guidelines, and recommended practices.
- **SITE ASSISTANCE AND EVALUATIONS** – ICS-CERT offers onsite field assessments, network design architectural reviews, and network traffic analysis and verification.

CONTACT ICS-CERT

For more information about ICS-CERT, please visit our web site: https://ics-cert.us-cert.gov/.

To contact ICS-CERT with a question, or to report a cyber incident, please send email to: ics-cert@hq.dhs.gov, or call: (877) 776-7585.